EXAMPLES OF PROOFWRITING FOR MATH 13 DISCUSSION PROBLEMS

OF THURSDAY, MARCH 10, 2016

The following are just examples of proofwriting. There are many other ways how to write these proofs correctly, so should consider these only as guidelines. The important point is that you justify each step and clearly explain which assumption/property is which is used and how it is used. You should be able to figure out on your own what to write and how much to write.

Problem 1(a). The domain of f is $\mathbb{N} \times \mathbb{N}$, so elements of the domain of f are ordered pairs $\langle a, b\rangle$ where $a, b \in \mathbb{N}$. The following equivalences hold for every ordered pair $\langle a, b\rangle \in \mathbb{N} \times \mathbb{N}$.

$$\langle a, b\rangle \in f^{-1}[E] \iff f(\langle a, b\rangle) \in E \iff a \in E$$

The first equivalence is an immediate consequence of the definition of the inverse image $f^{-1}[E]$. The second equivalence follows from the definition of function f. We thus have

$$f^{-1}[E] = \{\langle a, b\rangle \in \mathbb{N} \times \mathbb{N} \mid a \in E\} = \{\langle a, b\rangle \in \mathbb{N} \times \mathbb{N} \mid a \text{ is even}\}$$

This can also be equivalently expressed as follows:

$$f^{-1}[E] = E \times \mathbb{N},$$

because for every ordered pair $\langle a, b\rangle$,

$$\begin{aligned} \langle a, b\rangle \in E \times \mathbb{N} &\iff a \in E \wedge b \in \mathbb{N} \iff (a \in \mathbb{N} \wedge b \in \mathbb{N}) \wedge a \in E \\ &\iff \langle a, b\rangle \in \mathbb{N} \times \mathbb{N} \wedge a \in E. \end{aligned}$$

□

Problem 1(b). The following equalities hold:

$$\begin{aligned} g[\{\langle a, b\rangle \in D \mid a = 2\}] &= \{g(\langle a, b\rangle) \mid \langle a, b\rangle \in D \wedge a = 2\} = \{g(\langle 2, b\rangle) \mid (2, b) \in D\} \\ &= \{b \mid \langle 2, b\rangle \in D\} = \{b \mid b \text{ is divisible by } 2\} = E \end{aligned}$$

The first equality follows from the definition of the image $g[\{\langle a, b\rangle \in D \mid a = 2\}]$, the second equality follows since $(\langle a, b\rangle \in D \wedge a = 2) \iff \langle 2, b\rangle \in D$, the third equality follows from the definition of g, the fourth equality follows from the definition of D and the last equality follows from the definition of E. □

Problem 1(c). This is a generalization of Problem 1(b). Similarly as in 1(b) we have the following calculations:

$$\begin{aligned} g[\{\langle a, b\rangle \in D \mid a = d\}] &= \{g(\langle a, b\rangle) \mid \langle a, b\rangle \in D \wedge a = d\} = \{g(\langle d, b\rangle) \mid (d, b) \in D\} \\ &= \{b \mid \langle d, b\rangle \in D\} = \{b \mid b \text{ is divisible by } d\} \end{aligned}$$

The justifications are the same as in 1(b) above. □

Problem 1(d). The following equalities hold:

$$\begin{aligned} f[\{\langle a,b\rangle \in D \mid b = 24\}] &= \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in D \wedge b = 24\} \\ &= \{f(\langle a,b\rangle) \mid \langle a,24\rangle \in D\} \\ &= \{a \mid \langle a,24\rangle \in D\} = \{a \mid 24 \text{ is divisible by } a\} \\ &= \text{the set of all divisors of 24.} \end{aligned}$$

The first equality follows from the definition of the image $f[\{\langle a,b\rangle \in D \mid b = 24\}]$, the second equality follows since $(\langle a,b\rangle \in D \wedge b = 24) \iff \langle a,24\rangle \in D$, the third equality follows from the definition of f, the fourth equality follows from the definition of D and the last equality follows by an obvious reformulation. □

Problem 2, calculation of $f[Q]$ and $g^{-1}[f[Q]]$. The quadrangle Q consists for the following lines:

- $A = \{\langle x,y\rangle \mid \mathbb{R}\times\mathbb{R} \mid y = x+3 \wedge -2 \le x \le -1\}$
- $B = \{\langle x,y\rangle \mid \mathbb{R}\times\mathbb{R} \mid y = x-1 \wedge 0 \le x \le 1\}$
- $C = \{\langle x,y\rangle \mid \mathbb{R}\times\mathbb{R} \mid y = -x+1 \wedge -1 \le x \le 1\}$
- $D = \{\langle x,y\rangle \mid \mathbb{R}\times\mathbb{R} \mid y = -x-1 \wedge -2 \le x \le 0\}$

so $f[Q] = f[A \cup B \cup C \cup D]$. Regarding $f[Q]$:

$$\begin{aligned} f[Q] &= \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in Q\} \\ &= \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in A \vee \langle a,b\rangle \in B \vee \langle a,b\rangle \in C \vee \langle a,b\rangle \in D\} \\ &= \begin{array}{l} \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in A\} \\ \qquad \cup \ \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in B\} \\ \qquad \cup \ \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in C\} \\ \qquad \cup \ \{f(\langle a,b\rangle) \mid \langle a,b\rangle \in D\} \end{array} \\ &= \begin{array}{l} \{f(\langle a,b\rangle) \mid b = a+1 \wedge -2 \le a \le -1\} \\ \cup \ \{f(\langle a,b\rangle) \mid b = a-1 \wedge 0 \le a \le 1\} \\ \cup \ \{f(\langle a,b\rangle) \mid b = -a+1 \wedge -1 \le a \le 1\} \\ \cup \ \{f(\langle a,b\rangle) \mid b = -a-1 \wedge -1 \le a \le 0\} \end{array} \\ &= \begin{array}{l} \{a \mid b = a+1 \wedge -1 \le a \le -1\} \\ \cup \ \{a \mid b = a-1 \wedge 0 \le a \le 1\} \\ \cup \ \{a \mid b = -a+1 \wedge -1 \le a \le 1\} \\ \cup \ \{a \mid b = -a-1 \wedge -1 \le a \le 0\} \end{array} \\ &= [-2,-1] \cup [0,1] \cup [-1,1] \cup [-1,0] \\ &= [-2,1]. \end{aligned}$$

Here the first equality follows from the definition of the image $f[Q]$, the second equality follows from the breakup of Q into the union of A, B, C, D above, the third equality follows from the definition of the union of sets, the fourth equality follows from the definition of sets A, B, C, D, the fifth equality follows from the definition of f, and the remaining equalities are obvious.

Regarding $g^{-1}[f[Q]]$:

$$\begin{aligned} g^{-1}[f[Q]] &= g^{-1}[[-2,1]] = \{\langle a,b\rangle \in \mathbb{R}\times\mathbb{R} \mid g(\langle a,b\rangle) \in [-2,1]\} \\ &= \{\langle a,b\rangle \in \mathbb{R}\times\mathbb{R} \mid b \in [-2,1]\} \\ &= \mathbb{R} \times [-2,1] \end{aligned}$$

Here the first equality follows from the calculation of $f[Q]$ above, the second equality follows from the defintion of $g^{-1}[[-2,1]]$, the third equality follows from the definition of g and the last equality follows from the definition of Cartesian product. □

Problem 3(a). If A has only one element, say $A = \{a\}$ then $A \times A = \{\langle a, a\rangle\}$. In this case $\langle a, a\rangle = f(a)$, so every element of $A \times A$ is in $\mathsf{Im}(f)$. It follows that f is surjective.

If A has more than one element, say $a \neq b$ and $a, b \in A$ then $\langle a, b\rangle \in A \times A$ but $\langle a, b\rangle \notin \mathsf{Im}(f)$ because by the definition of f, if $y \in \mathsf{Im}(f)$ then $y = f(x)$ for some $x \in A$ and $f(x) = \langle x, x\rangle$. Hence if $y \in \mathsf{Im}(f)$ then the components of z are equal.

If $a, b \in A$ and $f(a) = f(b)$ then $\langle a, a\rangle = \langle b, b\rangle$ by the definition of f. Then $a = b$ since two ordered pairs are equal iff their first components are equal and also their second components are equal. We thus proved $f(a) = f(b) \implies a = b$, for all $a, b \in A$, so f is injective. □

Problem 3(c). (Problem 2(b) is similar – just think of the value b in 2(b) as the constant function $u : A \to B$ such that $u(a) = b$ for all $a \in A$.)

Injectivity of h: For each $a, a' \in A$ we prove $h(a) = h(a') \implies a = a'$:

$$h(a) = h(a') \implies \langle a, u(a)\rangle = \langle a', u(a')\rangle \implies a = a'$$

Here the first implication follows from the definition of h and the second implication follows because if two ordered pairs are equal then they have to agree on the first components. This proves injectivity of h.

Surjectivity of h: If B has precisely one element we prove that h is surjective. For this we need to prove that for every $y \in A \times B$ there is some $a \in A$ such that $h(a) = y$. (This is by the definition of surjectivity.)

Say $B = \{b\}$. Then $u(a) = b$ for all $a \in A$, as this is the only possibility for the value $u(a)$. Now pick $y \in A \times B$. We find $a \in A$ such that $h(a) = y$. As $y \in A \times B$, $y = \langle a, z\rangle$ for some $a \in A$ and $z \in B$. But since $B = \{b\}$ necessarily $z = b$, so $y = \langle a, b\rangle$. Above we saw that $b = u(a)$, so $y = \langle a, u(a)\rangle$. But $\langle a, u(a)\rangle = h(a)$ by the definition of h, so we just proved that $y = h(a)$, what was intended. This proves the surjectivity of h in the case where B has precisely one element.

If B has more than one element we prove that h is not surjective. We show that there is an element $y \in A \times B$ such that $y \notin \mathsf{Im}(h)$. Pick $a' \in A$. Since we assume B has more than one element, there is some $b' \in B$ such that $b' \neq u(a')$. We claim that $\langle a', b'\rangle \notin \mathsf{Im}(h)$, so the choice $y = \langle a', b'\rangle$ works. Why: Consider the values $h(a)$ where $a \in A$. If $a \neq a'$ then $h(a) = \langle a, u(a)\rangle \neq \langle a', b'\rangle$ because the two ordered pairs differ in their first components. If $a = a'$ then $h(a) = h(a') = \langle a', u(a')\rangle \neq \langle a', b'\rangle$ since the two ordered pairs differ in their second components. We thus proved that $\langle a', b'\rangle \neq h(a)$ for every $a \in A$, that is, $\langle a', b'\rangle \notin \mathsf{Im}(h)$. This proves that h is not surjective, as required. □

Problem 4(c). In order to prove that T is an equivalence relation, we need to prove that T is reflexive, symmetric and transitive.

Reflexivity: We need to prove that $\langle x, x\rangle \in T$ for all $x \in K \setminus \{0\}$. Now if $x \in K \setminus \{0\}$ then $x/x = 1 \in \mathbb{Q}$, so this is satisfied. This proves the reflexivity of T.

Symmetricity: We need to prove that for every $x, y \in K \setminus \{0\}$ the implication $\langle x, y\rangle \in T \implies \langle y, x\rangle \in T$ holds. Let $q = x/y$. Since we are assuming $\langle x, y\rangle \in T$, we have $q \in \mathbb{Q}$. But then also $1/q \in \mathbb{Q}$ since the ratio of two rational numbers is

rational. But $1/q = y/x$, so this shows that $y/x \in \mathbb{Q}$, as desired. This proves the symmetricity of T.

Transitivity: We need to prove that for every $x, y, z \in K \setminus \{0\}$ the implication $(\langle x, y\rangle \in T \ \wedge \ \langle y, z\rangle \in T) \implies \langle x, z\rangle \in T$ holds. By the definition of T, this amounts to showing the implication $(x/y \in \mathbb{Q} \ \wedge \ y/z \in \mathbb{Q}) \implies x/z \in \mathbb{Q}$. Now $x/z = (x/y) \cdot (y/z)$. Since the product of two rational numbers is rational, also $x/z \in \mathbb{Q}$, which we intended to prove. This proves the transitivity of T.

Now consider an arbitrary $x \in K \setminus \{0\}$. By the definition of equivalence class,

$$[x]_T = \{y \in K \setminus \{0\} \mid \langle x, y\rangle \in T\}$$

so

$$[x]_T = \{y \in K \setminus \{0\} \mid x/y \in \mathbb{Q}\}$$

Now notice that the following are equivalent:

- $x/y \in \mathbb{Q}$
- $y/x \in \mathbb{Q}$
- $x = y \cdot q$ for some $q \in \mathbb{Q}$
- $y = x \cdot q$ for some $q \in \mathbb{Q}$

This is because $x = y \cdot (x/y)$ and $y = x \cdot (y/x)$. So we can equivalently write:

$$[x]_T = \{q \cdot x \mid q \in \mathbb{Q}\}$$

or

$$[x]_T = \{y \in K \setminus \{0\} \mid x = q \cdot y \text{ for some } \ \in \mathbb{Q}\}$$

This describes the equivalence class $[x]_T$. □

Problem 4(d). In order to prove that T is an equivalence relation, we need to prove that V is reflexive, symmetric and transitive.

Reflexivity: We need to prove that $\langle a, a\rangle \in V$ for all $a \in P$. Since $a = a$, this is immediately true by the definition of V.

Symmetricity: We need to prove that the implication $\langle a, b\rangle \in V \implies \langle b, a\rangle \in V$ holds for all $a, b \in P$. If $a = b$ this conclusion is trivial, so assume $a \neq b$. Consider the following calculation:

$$\frac{b_1 - a_1}{b_0 - a_0} = \frac{(-1)(a_1 - b_1)}{(-1)(a_0 - b_0)} = \frac{a_1 - b_1}{a_0 - b_0}$$

It follows:

$$\langle a, b\rangle \in V \implies \frac{b_1 - a_1}{b_0 - a_0} = 1 \implies \frac{a_1 - b_1}{a_0 - b_0} = 1 \implies \langle b, a\rangle \in V$$

This proves the symmetricity of V.

Transitivity. We need to prove that for all points $a, b, c \in P$ the implication $(\langle a, b\rangle \in V \ \wedge \ \langle b, c\rangle \in V) \implies \langle a, c\rangle \in V$ holds. We may assume that a, b, c are all distinct, as otherwise the conclusion follows trivially. This will make the following calculations valid, as all differences in those calculations are non-zero. Now

$$\langle a, b\rangle \in V \implies \frac{b_1 - a_1}{b_0 - a_0} = 1 \implies b_1 - a_1 = b_0 - a_0$$

where the first implication follows from the definition of V and the second follows by multiplying both sides of the equation by $b_0 - a_0$. Similarly we get

$$\langle b, c\rangle \in V \implies \frac{c_1 - b_1}{c_0 - b_0} = 1 \implies c_1 - b_1 = c_0 - b_0$$

By adding the left/right sides of the two rightmost equations we get

$$(b_1 - a_1) + (c_1 - b_1) = (b_0 - a_0) + (c_0 - b_0)$$

hence

$$c_1 - a_1 = c_0 - a_0$$

and so

$$\frac{c_1 - a_1}{c_0 - a_0} = 1$$

which by the definition of V means that $\langle a, c\rangle \in V$. This completes the proof of transitivity of V.

Now we compute the equivalence class $[a]_V$. By the definition of V,

$$[a]_V = \{b \in P \mid \langle a, b\rangle \in V\}$$

By the definition of V this means

$$[a]_V - \{b \in P \mid a = b \ \vee \ \frac{b_1 - a_1}{b_0 - a_0} = 1\}$$

Now

$$a = b \ \vee \ \frac{b_1 - a_1}{b_0 - a_0} = 1 \iff b_1 - a_1 = b_0 - a_0 \iff b_1 - b_0 + (a_0 - a_1) = 0$$

So $b \in [a]_V$ iff b is the solution of the equation $y - x + (a_0 - a_1) = 0$. In other words, $b \in [a]_V$ iff b is a point on the line with equation $y - x + (a_0 - a_1) = 0$. This is the line which contains point a and has slope 1, that is, the angle with axis x is 45°. In conclusion,

$$\begin{array}{rcl} [a]_V & = & \text{the line containing the point } a \text{ with slope } 1 \\ & = & \text{the line containing the point } a \text{ which has angle } 45^\circ \text{ with axis } x. \end{array}$$

□

Problem 4(e). In order to prove that equinumerosity is an equivalence relation, we need to prove that it is reflexive, symmetric and transitive.

Reflexivity: We need to prove that if $A \in \mathcal{P}(U)$ then $A \sim A$. By the definition of equinumerosity, we need to find a bijection $f : A \to A$. Now the identity map $i : A \to A$ defined by $i(a) = a$ for every $a \in A$ is such a bijection. To see this, we verify that i is both injective and surjective. Regarding injectivity, if $a, b \in A$ then we have $a \neq b \implies i(a) \neq i(b)$ because $i(a) = a$ and $i(b) = b$. This verifies the injectivity of i. Regarding surjectivity, if $a \in A$ then $a = i(a)$ by the definition if i, hence $\mathsf{Im}(i) = A$. This proves that i is surjective. We have thus proved that $i : A \to A$ is bijective, so it suffices to let $f = i$. This proves that the relation of equinumerosity is reflexive.

Symmetricity. We need to prove for every $A, B \in \mathcal{P}(U)$ that if $A \sim B$ then $B \sim A$. By the definition of equinumerosity, this can be reformulated as follows:

$$(\exists f)(f : A \to B \wedge \ f \text{ is a bijection}) \implies (\exists g)(g : B \to A \wedge \ g \text{ is a bijection})$$

So assume $f : A \to B$ is a bijection and we find a bijection $g : B \to A$. We claim we can let $g = f^{-1}$. Recall that $f \subseteq A \times B$ and is a binary relation, so the expression f^{-1} makes sense. By the definition of f^{-1},

$$f^{-1} = \{\langle b, a\rangle \in B \times A \mid \langle a, b\rangle \in f\}$$

We first show that f^{-1} is a function from B to A, in other words $f^{-1} : B \to A$. We already know that $f^{-1} \subseteq B \times A$, so by the definition of function we need to verify that (i) for every $b \in B$ and $a, a' \in A$, the implication

$$(\langle b, a\rangle \in f^{-1} \wedge \langle b, a'\rangle \in f^{-1}) \implies a = a'$$

holds, and (ii) that for every $b \in B$ there exists some $a \in A$ such that $\langle b, a\rangle \in f^{-1}$. We first verify (i). By the definition of f^{-1}, the left side of this implication can be equivalently rewritten as

$$\langle a, b\rangle \in f \wedge \langle a', b\rangle \in f$$

Since we are assuming that f is bijective, f is injective, so this conjunction implies $a = a'$, which is what we wanted to prove. We thus proved the requirement (i) on f^{-1} being a function. To prove requirement (ii), pick any $b \in B$. Since f we are assuming that f is a bijection, f is surjective, so there is some $a \in A$ such that $\langle a, b\rangle \in f$. By the definition of f^{-1} this means that $\langle b, a\rangle \in f^{-1}$, which proves (ii). So we proved that f^{-1} is a function from A to B. Now we need to prove that f^{-1} is a bijection. We first prove that f^{-1} is injective. By the definition of injectivity this means to prove that for every $b, b' \in B$ and $a \in A$ the implication

$$(\langle b, a\rangle \in f^{-1} \wedge \langle b', a\rangle \in f^{-1}) \implies b = b'$$

holds. The left side of this implication can be rewritten as

$$\langle a, b\rangle \in f \wedge \langle a, b'\rangle \in f$$

Since f is a function from A to B, by the definition of function it follows that $b = b'$, which is what we needed to prove. So at the moment we proved that $f^{-1} : B \to A$ is an injection. To prove that $f^{-1} : B \to A$ is a bijection we need to prove that $f^{-1} : B \to A$ is surjective. By the definition of surjectivity, this means to prove the following: If $a \in A$ then there exists some $b \in B$ such that $\langle b, a\rangle \in f^{-1}$. Since $f : A \to B$ is a function, the value $f(a)$ is defined, so we can let $b = f(a)$. Then $\langle a, b\rangle \in f$, and by the definition of f^{-1} we have $\langle b, a\rangle \in f^{-1}$, which is what we needed to prove. So we proved that $f^{-1} : B \to A$ is surjective, and thereby that $f^{-1} : B \to A$ is a bijection. This completes the proof of symmetricity.

Transitivity. We need to prove that if $A, B, C \in \mathcal{P}(U)$ then the following implication holds:

$$(A \sim B \wedge B \sim C) \implies A \sim C$$

So consider A, B, C as above. Since we are assuming that $A \sim B$ and $B \sim C$, there exist bijections

$$f : A \to B \quad \text{and} \quad g : B \to C$$

We claim that $h = g \circ f : A \to C$ is a bijection. Once this is proved, this proves the transitivity. By the definition of composition, $h : A \to C$ is a function such that

$$h(a) = g(f(a))$$

for every $a \in A$. We need to verify that $h : A \to C$ is a bijection. First we verify the injectivity of h. By the definition of injectivity we need to verify that the implication

$$h(a) = h(a') \implies a = a'$$

holds for all $a, a' \in A$. Now

$$h(a) = h(a') \implies g(f(a)) = g(f(a')) \implies f(a) = f(a') \implies a = a'$$

Here the first implication follows from the definition of h, which gives that $h(a) = g(f(a))$ and $h(a') = g(f(a'))$. The second implication follows from the injectivity of g and the third implication follows from the injectivity of f. This completes the proof of injectivity of h. Now we need to verify that h is surjective. By the definition of surjectivity, we need to prove that if $c \in C$ is arbitrary then there exists some $a \in A$ such that $h(a) = c$. So pick $c \in C$. Since we are assuming $g : B \to C$ is bijective, $g : B \to C$ is surjective, so by the definition of surjectivity there exists some $b \in B$ such that $c = g(b)$. Since we are assuming that $f : A \to B$ is bijective, $f : A \to B$ is surjective, so again by the definition of surjectivity there exists some $a \in A$ such that $b = f(a)$. But then $c = g(b) = g(f(a)) = h(a)$, hence we found a as we needed. This proves that $h : A \to C$ is surjective, and thereby that $h : A \to C$ is bijective.

This also completes the proof of transitivity of equinumerosity, and thereby the proof that equinumerosity is an equivalence relation.

We now look at equivalence classes. If $A \in \mathcal{P}(U)$ then by the definition of an equivalence class,

$$[A]_\sim = \{B \in \mathcal{P}(U) \mid A \sim B\}$$

so $[A]_\sim$ consists of all sets in $\mathcal{P}(U)$ which are equinumerous to A, or in other words which have the same number of elements as A. □

As an example of good proofwriting of a proof in number theory, I am giving an example or writing the solution of Problem 3 in Homework 4. Please refer to the Homework 4 assignment sheet.

Regarding (G1), we want to prove that $d \,|\, a$ and $d \,|\, b$. Assume a contradiction this is false; so $d \nmid a$ or $d \nmid b$. We will only treat the case $d \nmid a$, as the case $d \nmid b$ is treated similarly. By the division algorithm there are numbers $q, r \in \mathbb{Z}$ such that

$$a = d \cdot q + r \quad \text{and} \quad 0 \leq r < d.$$

Since we are assuming $d \nmid a$, we have $r \neq 0$. So $0 < r < d$. Since $d = a \cdot x + b \cdot y$ where x, y are integers, by substituting in the formula above we have

$$a = (a \cdot x + b \cdot y) \cdot q + r = a \cdot x \cdot q + b \cdot y \cdot q + r$$

We now express r, so

$$r = a - a \cdot x \cdot q - b \cdot y \cdot q = a \cdot (1 - x \cdot q) + b \cdot (-y \cdot q)$$

Then $x' = 1 - x \cdot q$ and $y' = -y \cdot q$, are integers such that $r = a \cdot x' + b \cdot y'$. Since $0 < r < d$ this contradicts the minimality of d. It follows that $d \,|\, a$ after all.

Regarding (G2), assume $d' \,|\, a$ and $d' \,|\, b$. By the definition of divisibility, this means that there exist integers k, ℓ such that

$$a = d' \cdot k \quad \text{and} \quad b = d' \cdot \ell$$

Then

$$d = a \cdot x = b \cdot y = a \cdot d' \cdot k + b \cdot d' \cdot \ell = d' \cdot (a \cdot k + b \cdot \ell)$$

Since $a \cdot k + b \cdot \ell$ is an integer, this shows that $d' \,|\, d$. □